CyLaw-Report XXIX
ISSN: 1867-1969

TECHNISCHE UNIVERSITÄT DARMSTADT

V. Sauer / V. Schmid: Technische Hintergrundinformationen zur E-Justice (10/2009) im Rahmen der Kommentierung zu § 55a VwGO in Sodan/Ziekow, Kommentar zur Verwaltungsgerichtsordnung, 3. Auflage, 2010

Die CyLaw-Reports I-XIX wurden im Rahmen eines vom Bundesministerium für Bildung und Forschung geförderten Projekts (SICARI (2003 – 2007)) erstellt. Mit CyLaw-Report XX folgende wird dieses Online-Legal-Casebook vom Fachgebiet Öffentliches Recht an der Technischen Universität Darmstadt (Prof. Dr. Viola Schmid, LL.M. (Harvard)) fortgeführt. Die CyLaw-Reports sind keine „Living Documents", die ständig aktualisiert werden. Zitierungen können deswegen veraltet sein. Die Rechtfertigung für diese klassische Perspektive ist, dass den in den CyLaw-Reports präsentierten Entscheidungen der Gerichte nur die jeweils geltende Rechtslage zu Grunde gelegt werden konnte. Der Aufgabe der Aktualisierung stellt sich der Lehrstuhl in der integrierten Veranstaltung „Recht der Informationsgesellschaft". Hier wird das Methodenwissen von Studierenden der Technikwissenschaft so gefördert, dass sie in Übungen an der notwendigen Aktualisierung selbst mitwirken können.
Der vorliegende Cylaw-Report entstand im Rahmen einer Studienarbeit von Herrn Dipl.-Wirtsch.-Inform. Volker Sauer zur Unterstützung der Kommentierung zum § 55a VwGO in Sodan/Ziekow, Verwaltungsgerichtsordnung, 3. Auflage, demnächst.

A. Zur Sicherheit der in der E-Justice der BRD eingesetzten Übertragungsformate

Grundsätzlich gibt es in der E-Justice drei Möglichkeiten – basierend auf drei Protokollen –, elektronische Dokumente zu übertragen:

- Zunächst das OSCI-Protokoll, welches im EGVP-Verfahren und den entsprechenden Software-Produkten zum Einsatz kommt.
- Des Weiteren das SMTP-Protokoll, welches zum Einsatz kommt, wenn die zu übertragenden Schriftsätze per E-Mail versendet werden.
- Und das http-Protokoll, welches verwendet wird, wenn die zu übertragenden Schriftsätze mittels eines Upload-Formulars im Webbrowser über das WWW übertragen werden.

I. OSCI (EGVP)

Auf Anwenderseite berichtet die Firma Bremen Online Services von mittlerweile 35.000 OSCI-Nutzern auf der Nachfragerseite. OSCI (engl. für Online Services Computer Interface)

ist der Name eines Protokollstandards für die deutsche Kommunalwirtschaft. Er steht für mehrere Protokolle, deren gemeinsames Merkmal die besondere Eignung für das E-Government ist. OSCI-Transport-Nachrichten haben einen zweistufigen „Sicherheitscontainer". Dadurch ist es möglich, Inhalts- und Nutzungsdaten streng voneinander zu trennen und kryptographisch unterschiedlich zu behandeln. Die Inhaltsdaten werden vom Autor einer OSCI-Transport-Nachricht so verschlüsselt, dass nur der berechtigte Leser sie dechiffrieren kann. Die Nutzungsdaten werden vom Intermediär für die Zwecke der Nachrichtenvermittlung und die Erbringung der Mehrwertdienste benötigt, sie werden deshalb für den Intermediär verschlüsselt. Der Intermediär kann aber nicht auf die Inhaltsdaten zugreifen. Oft wird hier vom „Prinzip des doppelten Umschlages" gesprochen: Die verschlüsselten Inhaltsdaten sind wiederum in einen verschlüsselten Container eingebettet. Ein Angreifer kann wegen dieser Verschlüsselungen weder die Nutzungs- noch die Inhaltsdaten abhören.[1] In den Worten U. Berlits:[2] „Das EGVP ist eine Software, mit der Gerichte und Behörden mit ihren „Kunden" (z.B. Verfahrensbeteiligten, Antragstellern) und untereinander sicher unstrukturierte Nach-richten im OSCI-Format austauschen können; diese Nachrichten können vor allem mit An-hängen versehen und bei Bedarf mit einer qualifizierten elektronischen Containersignatur versehen werden."

Das EGVP wird als Java-Web-Start-Anwendung (läuft über den Browser) im Internet kostenfrei bereitgestellt. Der Aufwand ist nicht höher als bei der Nutzung des von der Steuerverwaltung angebotenen ELSTER-Programms.

Das EGVP selbst stellt an die Technik- und Kommunikationskompetenz der potentiellen Nutzer keine überspannten Anforderungen. Im Erscheinungsbild und der Handhabung ähnelt es gängigen E-Mail-Programmen. Auch wenn es nicht deren Funktionsumfang aufweist, entspricht die Erstellung einer EGVP-Nachricht in Ablauf und Aufwand im Kern der Erstellung einer E-Mail-Nachricht. Besonderheiten sind der Bindung der OSCI-Kommunikation an einen Intermediär und der Funktion geschuldet, die Kommunikation mit Gerichten und Behörden zu organisieren.

Über das EGVP können Nachrichten nicht unverschlüsselt versandt werden. Datenschutzverstöße durch Fehlbedienung sind insoweit ausgeschlossen. Ausgehende Nachrichten können signiert (qualifiziert oder fortgeschritten) oder unsigniert versendet werden; das entsprechende Signaturniveau kann bei der Nachrichtenerstellung festgelegt und bis zum Versand nachträglich geändert werden. Diese Festlegungen gelten nur für die Signatur des Nachrichtencontainers, in dem sich vorbehaltlich empfängerdefinierter Formatbeschränkungen beliebige, also auch signierte Anhänge befinden können. Die Signatur erfolgt aus dem EGVP heraus. Das EGVP setzt für die qualifizierte Signatur eine Signaturkarte voraus. Die Anwendung kann mit zahlreichen Karten und Kartenlesegeräten unter verschiedenen Betriebssystemen zusammenarbeiten.

Für den Empfänger der EGVP-Nachricht erfolgt eine zentrale Signaturprüfung (kryptographische Signaturprüfung und Zertifikatsprüfung), deren Ergebnis auf einem entsprechenden Prüfprotokoll festgehalten und mitgeteilt wird. Eine zentrale Virenprüfung auf dem Inter-

[1] Wikipedia, Online Services Computer Interface, Version vom 30.10.2009, 15.57 Uhr, http://de.wikipedia.org/w/index.php?title=Online_Services_Computer_Interface&oldid=66201215. Vgl. zur Zitierweise von Wikipedia R. Zosel, Im Namen des Volkes: Gerichte zitieren Wikipedia, JurPC Web-Dok. 140/2009, http://www.jurpc.de/aufsatz/20090140.htm.

[2] U. Berlit, Das Elektronische Gerichts- und Verwaltungspostfach bei Bundesfinanzhof und Bundesverwaltungsgericht, JurPC Web-Dok. 13/2006, http://www.jurpc.de/aufsatz/20060013.htm, Rn. 12.

mediär erfolgt derzeit auf Wunsch der das EGVP einsetzenden Gerichte nicht; hierfür müsste die Nachricht jedenfalls kurzzeitig unverschlüsselt auf dem Intermediär vorliegen, was bei dem Grunde nach unterstellter Zulässigkeit erhöhte Anforderungen an den Betreiber des Intermediärs stellte. Für den Versender der Nachricht wird ein Sendeprotokoll erstellt, das neben einem Nachrichtenkennzeichen u.a. Absender und Empfänger der Nachricht sowie Dateiname, -datum und -größe einer übermittelten Nachricht enthält. Eine vom Intermediär während des Sendevorgangs an den Absender übermittelte Eingangsbestätigung weist Absender und Empfänger der Sendung, Betreff und - sekundengenau - das Ende des Empfangsvorganges auf dem Server des Intermediärs aus; da sich die Nachricht selbst verschlüsselt in einem Container befindet, können in dieses „Empfangsbekenntnis“ keine - überprüften - Angaben zum Inhalt der Nachricht aufgenommen werden. Aus Kostengründen wurde davon abgesehen, für die Eingangsbestätigung qualifizierte Zeitstempel einzusetzen; die Zuverlässigkeit der Zeitangabe braucht nicht höher als etwa bei gerichtlichen Nachtbriefkästen zu sein.
Der Nachrichtenempfang gestaltet sich ähnlich wie ein E-Mail-Empfang. Die Nachrichten müssen vom Intermediär abgeholt werden; dabei werden sie automatisch entschlüsselt und für das Posteingangsfenster „aufbereitet“.
Im Posteingangsfenster werden in einem Übersichtsbereich die wesentlichen Informationen zu einer Nachricht aufgelistet, darunter auch das Ergebnis der Signaturprüfung. Detailangaben zu der eingegangenen Nachricht können über Registerblätter abgerufen werden. Hervorzuheben ist das Prüfprotokoll, das detaillierte Angaben zu der empfangenen Nachricht und dort insbesondere das Ergebnis der Signatur- und Signaturzertifikatsprüfung enthält; wurden mit der signierten OSCI-Nachricht Dokumente versandt, die vom Sender signiert wurden, werden auch diese Zertifikate überprüft und in einem gesonderten Registerblatt die Ergebnisse dargestellt. Das allgemeine Prüfprotokoll ist bei einer weiterhin führenden Papierakte Grundlage des vom Gesetzgeber vorgeschriebenen Transfervermerks, der auf dem Ausdruck anzubringen ist. Nachricht, Anhänge und Protokoll können ausgedruckt werden.
Das OSCI-Protokoll wird nicht nur von der EGVP Software implementiert, sondern kann auch von anderen Herstellern implementiert werden. So z.B. von Herstellern von Anwalts-Bürosoftware wie der Firma RA-Micro. Manche Anwälte nutzen EGVP über die Software RA-Micro mit einer Chipkarte. Diese Chipkarten können bei der Rechtsanwaltskammer beantragt und per Post in Empfang genommen werden.

II. SMTP(S) (E-Mail)

1. SMTP

SMTP (Simple Mail Transfer Protocol) ist das Protokoll, welches für den Transport von E-Mail im Internet verantwortlich ist. Es arbeitet nach dem Store-and-Forward-Prinzip, so dass Nachrichten über Zwischenknoten, die die Nachrichten temporär speichern, weitergeleitet werden, bis sie schließlich in der Mailbox des Empfängers abgelegt werden.[3] Eine Weiterleitung einer Mail über mehrere (mehr als 2) Rechner ist dabei im heutigen Internet die Regel.

[3] C. Eckert, IT-Sicherheit, 2008, S. 145.

FEX: Der Zugriff auf die Mailbox des Empfängers durch ein E-Mail-Programm auf dem Rechner des Empfängers geschieht nicht mittels des SMTP-Protokolls, sondern meist über die Protokolle POP3 oder IMAP (z.B. bei MS Outlook/Exchange), die nicht Gegenstand dieser Betrachtung sind. Die Transportsicherheit und -authentizität kann bei POP3 und IMAP jedoch durch die entsprechenden Varianten POP3s und IMAPs zwischen dem Mailserver, welcher die Empfängermailbox beherbergt, und dem Rechner des Empfängers sichergestellt werden.

Drei wesentliche Sicherheitsprobleme können beim Einsatz vom SMTP entstehen:

(1) Die Mails werden unverschlüsselt über das Netz übertragen und können (wie jede andere unverschlüsselte Kommunikation im Internet) relativ leicht über frei verfügbare Sniffer-Programme abgehört werden.[4]

(2) Die Mails werden auf dem Vermittlungsrechnern unverschlüsselt abgelegt und können dort zumindest durch das Wartungspersonal der Rechner leicht mitgelesen werden.

(3) Die Absenderadressen von Mails können leicht gefälscht werden. Eine Authentizität der Mails wird durch SMTP nicht gewährleistet.

2. SMTPS

SMTP kann mittels SSL oder TLS zu SMTPS erweitert werden. Dies behebt jedoch nur das Problem (1) der Transportsicherheit. Durch die stattfindende Verschlüsselung kann die einzelne SMTPS-Verbindung zwischen den beteiligten Servern nicht mehr abgehört werden. Auch die Authentizität der beteiligten Server lässt sich mittels SMTPS sicherstellen – nicht jedoch die Authentizität der Mail selbst, so dass Problem (3) durch den Einsatz von SSL/TLS nicht gelöst wird.
Auch das Problem (2) wird durch SMTPS nicht behoben, da SMTPS nur **zwischen** Servern eingesetzt wird und Mails daher nach wie vor unverschlüsselt zwischengespeichert werden.
Fazit: SMTPS bietet somit nur eine **Punkt-zu-Punkt**-Sicherheit – keine Ende-zu-Ende-Sicherheit.

SMTPS ist bisher nicht weit verbreitet. Die meisten Server verwenden nach wie vor nur SMTP. Grund dafür könnte z.B. das Fehlen einer kostengünstigen und allgemein anerkannten Certificate Authority (CA) sein, die die für eine einwandfreie Authentizität der SMTPS-Verbindung notwendigen Zertifikate ausstellt. Ferner dürften auch die Komplexität des Themas bzw. die mangelenden Kenntnisse der meisten Administratoren Gründe für die geringe Verbreitung von SMTPS sein.

[4] Zum Risiko einer Strafbarkeit § 202c StGB.

3. Ende-zu-Ende-Sicherheit

Wird für E-Mails eine **Ende-zu-Ende**-Sicherheit gewünscht, ist statt oder zusätzlich zu SMTPS eine kryptographische Behandlung der E-Mail auf dem Rechner des Senders sowie des Empfängers notwendig.
Zur besseren Übersicht wird in diesem Falle zwischen den Sicherheitsmerkmalen der Vertraulichkeit (realisierbar durch Verschlüsselung) und Authentizität (realisierbar durch Signaturen) differenziert:

a) Authentizität

Die Authentizität einer E-Mail kann sichergestellt werden, indem der Sender der Mail diese mit einem kryptographischen Verfahren mit einer digitalen Signatur versieht. Der Empfänger der Mail prüft diese Signatur mit dem zugehörigen Prüfverfahren und kann so zunächst erkennen, ob die Mail während ihres Transportes modifiziert wurde. Ist dem Empfänger das sog. CA-Zertifikat bekannt, mit dessen Key das persönliche Zertifikat des Senders signiert wurde, und ist dieses CA-Zertifikat für den Empfänger vertrauenswürdig, so kann der Empfänger auch prüfen, ob die Mail wirklich vom angegebenen Sender stammt, also vertrauenswürdig ist. Problem (3) wird dadurch gelöst. Man spricht hier von einem transitiven Vertrauensverhältnis.
Voraussetzung für solche transitiven Vertrauensverhältnisse ist das Vorhandensein mindestens einer gemeinsamen zentralen vertrauenswürdigen Stelle, meist als CA (Certificate Authority) bezeichnet. Die Zertifikate dieser CAs nennen sich CA-Zertifikate. Echtheit und Vertrauen in diese sind essentiell für das Funktionieren des gesamten Vertrauensmodell. Die technische Infrastruktur, die eine solche CA betreibt wird meist PKI (Public Key Infrastruktur) genannt. CA- Zertifikate können in hierarchischen Ketten organisiert sein. Die Wurzel einer solchen Kette wird Root-Zertifikat genannt.
Die Signierung von Mails ist in der E-Justice vorgeschrieben. Welche CAs dabei verwendet werden und wie sichergestellt ist, dass die teilnehmenden Gerichte mit den entsprechenden CA-Zertifikaten, die Anwälte und Notare verwenden, ausgestattet sind und wie (technisch und organisatorisch) gewährleistet wird, dass die E-Justice E-Mail nicht durch falsche (CA-) Zertifikate kompromittiert werden kann, wurde im Rahmen dieser Arbeit nicht untersucht. Hier bestünde sicherlich für kommende Kommentare aufgrund der nach wie vor (trotz der großen Verbreitung von EGVP) noch vorhandenen Akzeptanz von E-Mail durch deutsche Gerichte noch weiterer Recherchebedarf.

b) Vertraulichkeit

Die Vertraulichkeit der E-Mails kann durch Verschlüsselung sichergestellt werden. Um eine Mail so zu verschlüsseln, dass nur deren legitimer Empfänger diese entschlüsseln kann, benötigt der Sender ein Zertifikat des Empfängers (genauer: den im Zertifikat enthaltenen Public-Key). Um die Echtheit des Zertifikats des Empfängers prüfen zu können (um so sicherzustellen, dass es sich beim angegebenen Empfänger wirklich um den „echten“ Empfänger handelt (siehe dazu auch die Ausführung zum Thema Authentizität; an dieser Stelle wird die Authentizität des Zertifikates des Empfänger gefordert)), wird das CA-Zertifikat des Empfängers benötigt. Ist über dieses Zertifikat die Echtheit des Empfängers sichergestellt, so kann

der Sender die Mail verschlüsseln und nur der echte Empfänger ist in der Lage, die Mail zu entschlüsseln. Das Problem (2) wird so gelöst.
Hinsichtlich des Einsatzes in der E-Justice lässt sich feststellen, dass für die optionale Verschlüsselung auf den Webseiten der Gerichte häufig eigene Zertifikate zum Download angeboten werden, welche von den Mail-Sendern zur Verschlüsselung der Nachrichten verwendet werden sollen. Wie hier sichergestellt wird, dass keine falschen Zertifikate in Umlauf geraten bzw. wie die teilnehmenden Anwälte und Notare genau dies verifizieren können, wäre noch zu recherchieren. (Für das Beispiel OVG RLP und dessen Probleme siehe Anhang).

c) Fazit

Nur eine Ende-zu-Ende-Verschlüsselung und Signierung beim Sender mittels Zertifikaten löst die Probleme 1-3 vollständig. Das Vorhandensein von (partieller) Transportsicherheit mittels SMTPS zwischen den Mailservern ist dabei unerheblich. Inwieweit die Verteilung und Sicherstellung der Echtheit der Zertifikate zur Mail-Verschlüsselung bei deutschen Gerichten gelöst ist, bliebe noch zu recherchieren. Eine optimale Lösung wäre die Ausstellung von Zertifikaten auf Chipkarten durch eine authentizierende und legitimierende Stelle wie der Anwalts- oder Notarkammer bei EGVP. Unter B. wird verdeutlicht, wie gefährlich die Nutzung von Zertifikaten aus unsicherer Quelle sein kann.

III. HTTP(S) (Web-Upload)

Eine HTTP(S)-Verbindung ist grundsätzlich eine **Punkt-zu-Punkt**-Verbindung zwischen dem (Web-)Server und dem (Web-)Client (Browser). Ein Store-and-Forward-Prinzip wie bei E-Mail ist hier zunächst nicht gegeben. Für diese HTTP(S)-Verbindung gelten die gleichen Aussagen wie oben zu SMTP(S) aufgeführt: Sicherheit lässt sich zwischen Client und Server durch den Einsatz von SSL/TLS erzielen.
Auch hier ist zu beachten, dass nur bei Echtheit der für HTTP(S) eingesetzten Zertifikate eine sichere Verbindung bestehen kann. Die gängigen Browser (Internet Explorer, Firefox etc.) enthalten dazu schon eine ganze Reihe von CA-Zertifikaten der großen Zertifizierungsstellen, denen der Nutzer implizit durch die Installation des Browsers vertraut.[5]
Hinsichtlich der Authentizität kann der Benutzer, der eine Datei hochlädt, über die Speicherung des Usernamens, den er beim Upload in ein Web-Formular eingetragen hat, authentifiziert und identifiziert werden. Alternativ wäre zusätzlich natürlich eine weitere Signierung und/oder Verschlüsselung der hochgeladenen Dateien denkbar. Genau wie bei SMTP(S) ist dies jedoch nicht Gegenstand des HTTP(S)-Protokolls, sondern letztlich der Anwendung, die die hochgeladenen Dateien (weiter-)verarbeitet.

[5] Viele Experten halten dieses Vertrauen für trügerisch, da durch die Installation eines gehackten Browsers, den der Benutzer z.B. aus dubioser Quelle installiert hat, dem Benutzer gefälscht CA-Zertifikate untergeschoben werden können und somit seine verschlüsselte Kommunikation z.B. über eine Man-In-the-Middle-Attack leicht abgehört werden kann, wobei sich der Benutzer durch die Verschlüsselungsanzeige im Browser (z.B. kleines Schloss o.ä.) sogar in Sicherheit wiegt, eine vertrauliche Kommunikation zu führen.

1. Spezialfall: OSCI-Gateway

Laut der „Kurzübersicht der Internetbekanntgabe zum elektronischen Rechtsverkehr im Land Hamburg“ zur Verordnung vom 28. Januar 2008 betreibt das Finanzgericht Hamburg bzw. dessen Dienstleister ein sogenanntes „Gateway“. Nach Auskunft der Firma Bremen-Online-Services, dem Hersteller der auf diesem Gateway eingesetzten Software „erv-d“, überführt dieses Gateway den Web-Upload des Benutzers in das OSCI-Protokoll und damit in das reguläre EGVP-System des Gerichts.
In diesem Gesamtsystem scheint daher doch das **Store-and-Forward**-Paradigma implementiert zu sein. Im ersten Schritt wird die zu übertragende Datei per HTTP(S) auf das Gateway übertragen. Die Sicherheit wird durch den Einsatz von SSL/TLS und User/Passwort gewähr-leistet. Die übertragenen Dokumente werden auf dem Gateway zwischengespeichert und dann in das OSCI-System weitergeleitet. Hier kommen dann vermutlich die üblichen OSCI-Sicherheitsmaßnahmen zum Einsatz.
Inwieweit in Hamburg mittels Signierung und Verschlüsselung eine **Ende-zu-Ende**-Sicherheit machbar ist, geht aus den öffentlichen Unterlagen nicht hervor. Zumindest die Signierung ist vorgeschrieben. Kommt keine solche Technik zum Einsatz, so wären die eingereichten Schriftsätze nach der Übertragung per HTTP(S) und vor der Weiterleitung per OSCI auf dem Gateway unverschlüsselt und evtl. sogar unsigniert. Das Gesamtsystem wäre dann nur noch so sicher, wie das Gateway selbst. Dringt ein Angreifer erfolgreich in das Gateway ein, wäre er in der Lage, alle Schriftsätze zu lesen und ggf. sogar unbemerkt zu modifizieren. Auch die Integrität des mit dem Betrieb des Gateways beauftragen Dienstleisters muss zum sicheren Betrieb des Gesamtsystems gewährleistet sein.

2. eGerichtsbriefkasten

Das von den Gerichten im Land Brandenburg sowie von BGH und BPatG genutzte System (letzter nutzen dieses System exklusiv) für elektronischen Rechtsverkehr per Web-Upload nennt sich „eGerichtsbriefkasten“ und ist über http://www.gerichtsbriefkasten.de/ im Internet erreichbar. Die Login-Seite des eGerichtsbriefkastens ist über ein SSL-Zertifikat, ausgestellt von der Firma Equifax Secure Inc., gesichert (Screenshot siehe Anhang). Das zugehörige CA-Zertifikat ist in allen gängigen Browser bereit vorhanden. Geht man davon aus, dass diese Zertifikate echt sind,[6] so ist mit dem eGerichtsbriefkasten eine sichere Kommunikation möglich. Die Authentifizierung des Benutzers erfolgt per Username/Passwort, welche der Benutzer nach vormaliger Anmeldung erhält. Die Anmeldung wird per Freischaltcode auf das Handy authentifiziert.
Die o.g. Webseite, über welche die Dokumente an die spezifizierten Gerichte hochgeladen werden können, wird von einer Firma AM-Soft GmbH aus Potsdam betrieben. Die IP-Adresse des Upload-Servers login.elrev.net (derzeit 83.218.37.3) ist laut der zuständigen Address-Registrierungsstelle „RIPE“ derzeit in Hameln, Niedersachsen, beim Provider Witte Bürotechnik GmbH lokalisiert. Wie die auf diesen Server hochgeladenen Dokumente an die teilnehmenden Gerichte weitergeleitet werden ist unklar.
Laut der auf http://www.gerichtsbriefkasten.de/ verfügbaren Kurzanleitung werden bestimmte Dokumente, z.B. die Klageschrift selbst, mittels einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen. Verwendbar seien z.B. die Signaturprodukte der deut-

[6] Zu Manipulationsmöglichkeiten siehe oben Fußnote 5.

schen Telekom, von D-Trust oder der Deutschen Post, die standardkonforme PKCS#7 Signaturen erzeugen können. Inwieweit das bedeutet, dass das System beim Upload die Signierung vornimmt oder etwa eine durch den User vorgenommene Signierung prüft, wird aus der Kurzanleitung nicht klar.
Auch in diesem System bleibt unklar, wie **die Ende-zu-Ende**-Sicherheit beim notwendigen Store-and-Forward vom HTTP-Server zu den Systemen des Gerichts sichergestellt ist. Zumindest die Authentizität nach Signaturgesetz scheint sichergestellt zu sein. Über eine mögliche Verschlüsselung ist in der Anleitung zum eGerichtsbriefkasten nichts zu finden. Ferner gelten auch beim eGerichtsbriefkasten alle Schwächen, die zum HTTP(S)- und SMTP(S)-Protokoll aufgeführt wurden (siehe oben Fußnote 5).

3. Fazit

Es ist deutlich erkennbar, dass OSCI (und damit des EGVP) ein Protokoll ist, welches speziell für den Einsatz im E-Government entwickelt wurde. Viele der Probleme, die beim Einsatz der (z.T. sehr alten) Protokolle HTTP (erstmalig 1996 standardisiert) und SMTP (erstmalig 1982 (!) standardisiert) entstehen, werden durch OSCI gelöst. Die von U. Berlit (Fn.2) aufgeführten Vorteile

> (1) Tatsache und Zeitpunkt des Transfers werden sehr zuverlässig und mit der Möglichkeit sofortiger Eingangsbestätigung protokolliert.
>
> (2) Die Vertraulichkeit des Transfers ist ohne zusätzliche Vorkehrungen zwingend gesichert, versehentlich unverschlüsselte Kommunikation ist ausgeschlossen.
>
> (3) Die Entlastung der Nutzer davon, die für die kryptographische Behandlung und die Signaturprüfung erforderlichen Vorkehrungen selbst treffen bzw. vorhalten zu müssen.

sollen das OSCI/EGVP-System zu einer ausgereiften und sicheren Anwendung machen. Insbesondere in Kombination mit Chipkarten kommt Argument 3 in o.g. Liste von U. Berlit zum Tragen und verhindert den in sämtlichen anderen Szenarien problematischen Umgang mit Zertifikaten. Generell ist der Einsatz von OSCI statt SMTP(S), HTTP(S) oder ggf. weiteren Protokollen anzuraten. SMTP und HTTP sind auf Transportebene zwar mittels SSL/TLS absicherbar, jedoch wirft die Ende-zu-Ende-Sicherheit nach wie vor Probleme auf, die OSCI durch den zweistufigen Sicherheitscontainer löst. Hybrid-Lösungen wie das HTTP-OSCI-Gateway (erv-d Software der Firma Bremen Online Services) mögen kurzfristig für eine höhere Akzeptanz des ERVs sorgen, sind jedoch sicher kein vollwertiger Ersatz für einen echten OSCI-Client.

B. Kritik an der Zertifikateverwendung beim E-Gerichtsbriefkasten

Bis Oktober 2008 war das Zertifikat des OVG Rheinland Pfalz (damals unter http://cms.justiz.rlp.de/justiz/nav/68e/68e10e74-db89-0f01-33e2-dc6169740b3c,,,,fff70331-6c7f-90f5-bdf3-a1bb63b81ce4.htm) von der T-Systems International GmbH ausgestellt. Dies lässt sich leicht durch den Download der Datei und durch Analyse mittels OpenSSL zeigen:

openssl x509 -inform der -text -in Gerichtsbriefkasten_OVG_Rheinland_Pfalz.cer:

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 14626 (0x3922)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=DE, O=T-Systems Enterprise Services GmbH, OU=Trust Center Deutsche Telekom, CN=MailPass CA

Validity

Not Before: Dec 10 07:59:11 2007 GMT

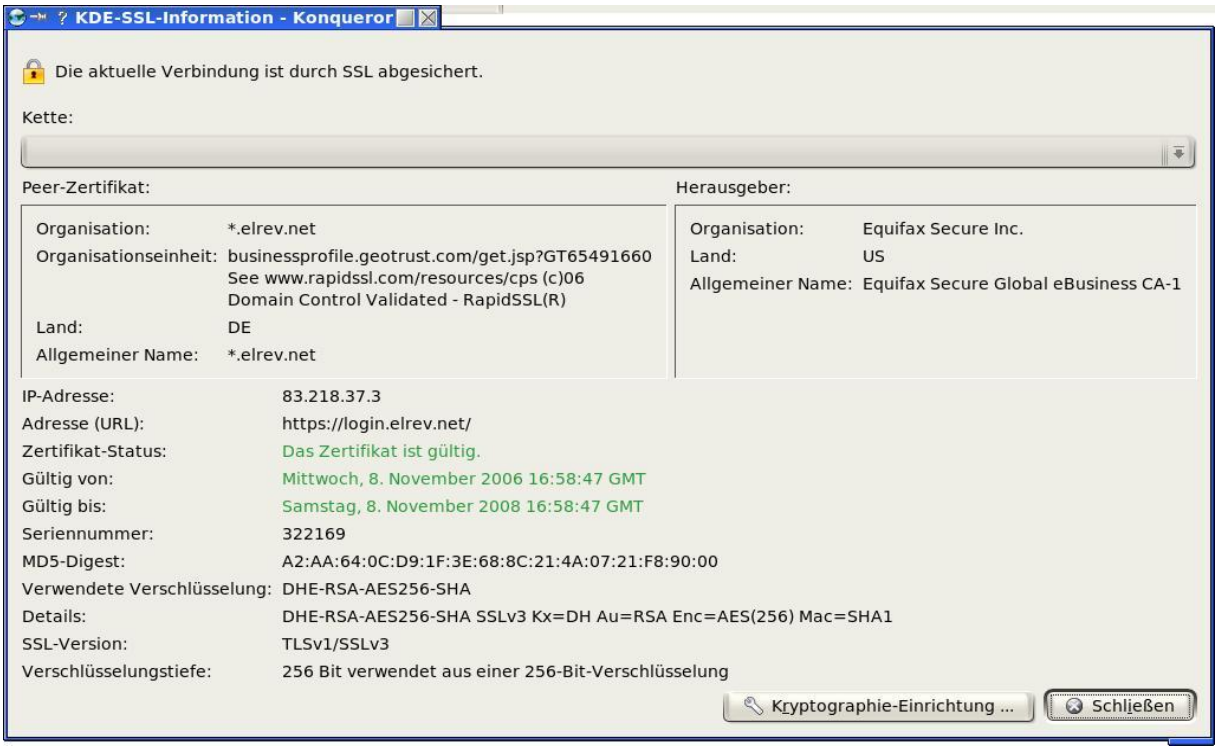
Not After : Dec 10 23:59:00 2008 GMT

Subject: C=DE, O=T-Systems International GmbH, OU=telesec.de, OU=Extern.telesec.de, OU=Oberverwaltungsgericht Rheinland-Pfalz, CN=Poststelle OVG Rheinland-Pfalz/emailAddress=gbk.ovg@ovg.jm.rlp.de

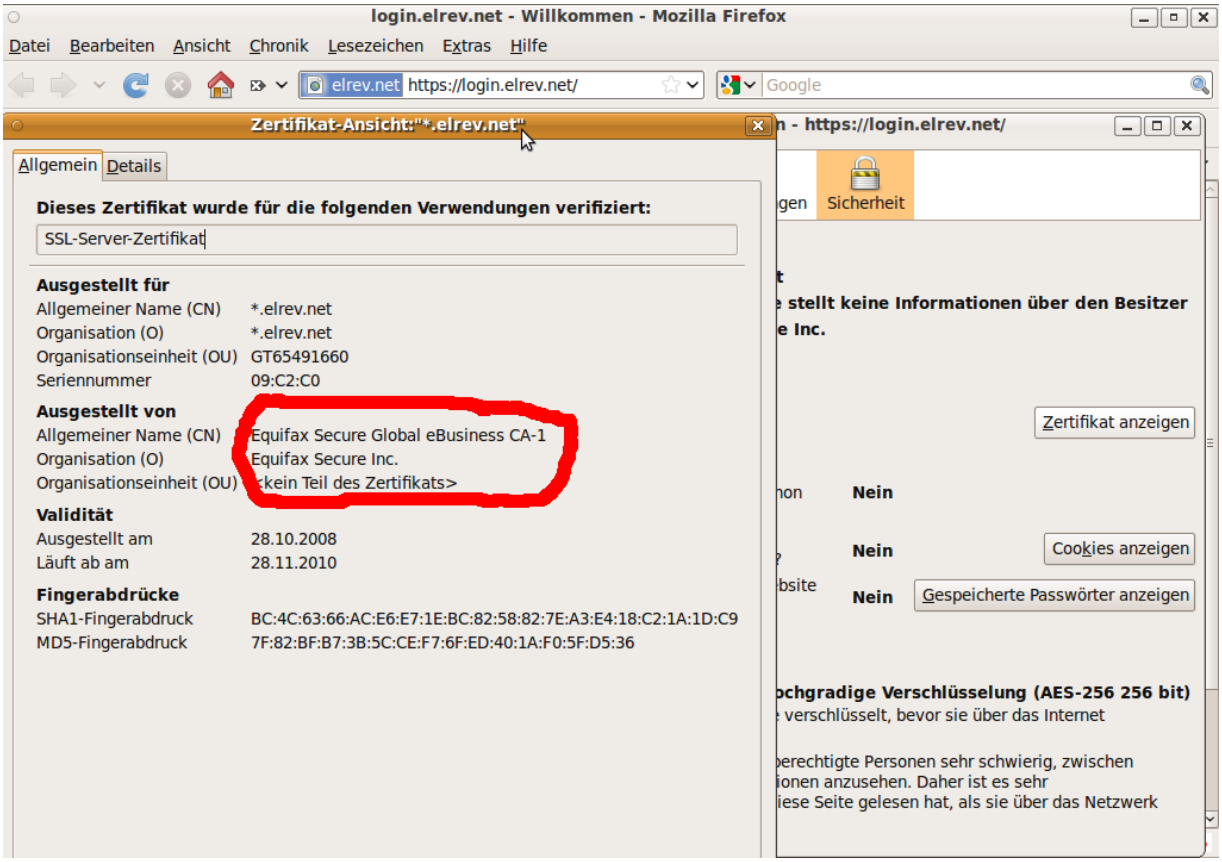
[...]

Das ausstellende CA-Zertifikat der T-Systems International GmbH (CN=MailPassCA) ist derzeit in den Produkten der Mozilla-Foundation (Mozilla, Firefox, Thunderbird etc.) nicht enthalten. Auch im Internet Explorer in den Versionen 6, 7 und 8 ist es nicht enthalten.
Möchte ein Anwalt also prüfen, ob das auf den Seiten des OVG zur Verfügung gestellte Zertifikat echt ist, kann er dies nur durch folgende zusätzliche Schritte tun: Er muss auf das entsprechende Zertifikat im Internet suchen. Unter www.telesec.de (Die Seite kann der Anwalt nur durch Studium des Zertifikates selbst, hier: Subject des Zertifikates, herausfinden.) ist dieses CA-Zertifikat jedoch nicht zu finden. Wäre es irgendwo aufzufinden, so müsste der Anwalt das Zertifikat installieren und dann den digitalen Fingerprint des Zertifikats auf sicherem Wege – d.h. entweder über eine signierten Webseite, dessen Signatur der Anwalt prüfen kann (weil er das entsprechende CA-Zertifikat besitzt und diesem vertraut) oder per Telefon durch einen Anruf bei der CA – mit dem offiziellen Fingerprint des CA-Zertifikats vergleichen. Nur bei Übereinstimmung ist das Zertifikat echt und kann für verschlüsselte Kommunikation verwendet werden.
Verzichtet der Anwalt auf diese Schritte und vertraut dem Zertifikat des OVG RLP „blind“, wäre es für einen Angreifer einfach (z.B. durch einen Einbruch in den Webserver des OVG RLP), das dortige Zertifikat durch ein anderes zu ersetzen und fortan die verschlüsselte Post des Anwaltes mitzulesen.
Hier wird deutlich, wie schwierig die Sicherheit von E-Mail sein kann, wenn eine vertrauenswürdige CA mit entsprechenden sicheren Geschäftsprozessen fehlt. Inwieweit ein Jurist ohne (vertieftes) Informatikwissen beim Fehlen einer solchen Stelle die Sicherheit selbst sicherstellen kann, sei dahingestellt.

Zertifikat von http://www.gerichtsbriefkasten.de bzw. der Login-Seite https://login.elrev.net



Seit Oktober 2009 hat der Betreiber der Seite https://login.elrev.net reagiert und das Zertifikat durch ein neues ersetzt:



Das neue Zertifikat wurde von „Equifax Secure Inc." unterzeichnet. Das zugehörige CA-Zertifikat ist in allen aktuellen Browsern enthalten. Vorbehaltlich der in FN 5 erwähnten Authentizität des Browser bzw. dessen mitgelieferten Zertifikaten ist somit eine sichere Kommunikation mit login.elrev.bet auch dem IT-Laien möglich.

C. Glossar

ASCII

Abkürzung für „American Standard Code for Information Interchange".[7] Der erste echte IT-Standard aus dem Jahre 1963 zur Übertragung von 128 lateinischen, alphanumerischen Zeichen der US-amerikanischen Schreibmaschinentastatur über Telekommunikationsverbindungen.[8] Für eine Tabelle mit ASCII Zeichen siehe Patterson/Hennessy, S. 142 oder Wikipedia, American Standard Code for Information Interchange, Version vom 14.12.2009, 13.13 Uhr, http://de.wikipedia.org/w/index.php?title=American_Standard_Code_for_Information_Interchange&oldid=67999268.

HTML

Abkürzung für „HyperText Markup Language". Ursprünglich zur Strukturierung und Verknüpfung der am CERN[9] anfallenden Datenmengen entwickelt,[10] ist HTML seit ca. 1990 die mittlerweile standardisierte[11] Beschreibungssprache zu Definition des Layouts aller Seiten des „World Wide Web" (WWW)[12] und damit die zentrale Komponente zur Bereitstellung und Verknüpfung verschiedener Dienste im Internet.[13]

HTTPS

ist das mittels SSL/TLS[14] abgesicherte Protokoll HTTP. HTTP bedeutet „Hypertext Transfer Protocol". Es handelt sich dabei um das Standardübertragungsprotokoll für WWW-Inhalte (z.B. HTML-Seiten) im Internet, wurde aber absichtlich allgemeiner ausgelegt, so dass auch beliebige andere Dateien übertragen werden können. Auch Datei-Uploads sind über HTTP möglich.[15] Mittels HTTPS ist durch eine positive Empfangsbestätigung auch eine verbindliche Übertragung realisierbar.

[7] Piepenbrock, Beck´scher TKG-Kommentar, Teil C, Glossar.
[8] G.S. Robinson/C. Cargill.
[9] „Conseil Europeen pour la Recherche Nucleaire", eine Großforschungseinrichtung in Genf in der Schweiz, an der physikalische Grundlagenforschung betrieben wird.
[10] T. Berners-Lee.
[11] T. Berners-Lee/D. Connolly.
[12] A. S. Tanenbaum, S. 683.
[13] C. Eckert, S. 130ff; siehe auch A. H. Horns, GRUR 2001, S. 14 ff.
[14] Siehe SSL/TLS.
[15] A. S. Tanenbaum, S. 706 f.

ISIS-MTT/Common PKI

Common PKI (vormals ISIS-MTT für Industrial Signature Interoperability and Mail-trust Specification) ist eine gemeinsam von der T7-Gruppe und TeleTrusT verabschiedete Spezifikation über international verbreitete und anerkannte Standards für elektronische Signaturen, Verschlüsselung und Public-Key-Infrastrukturen.[16] Die Ergebnisse werden im Internet zur freien Nutzung bekannt gegeben unter www.t7-isis.de.

Makro

Unter einem Makro versteht man eine bestimmte vorprogrammierte Befehlsfolge (z.B. Aktionen oder Tastaturcodes), welche innerhalb eines anderen Programms wie einer Textverarbeitung oder Tabellenkalkulation unter bestimmten Bedingungen (wie z.B. beim Öffnen des Dokuments, welches das Makro enthält) ausgeführt wird.[17]

Oasis OpenDocument (auch ODT)

ODT ist die Abkürzung von „OpenDocument Text". ODT ist Teil des „OASIS OpenDocument Format for Office Applications". Es handelt sich um einen offenen ISO-Standard[18] für Dateiformate von Bürodokumenten wie Texten, Tabellendokumenten, Präsentationen, Zeichnungen, Bildern und Diagrammen. Der „OpenDocument" Standard wird z.B. von OpenOffice und anderen OpenSource-Textverarbeitungen verwendet. Ab Service Pack 2 soll auch Microsoft Office 2007 diesen Standard unterstützen.[19]

OpenSource (Software)

OpenSource (Software) im weiteren Sinne ist Software, deren Quelltext[20] bei der Weitergabe der Software zur Verfügung gestellt wird. Im engeren Sinne ist OpenSource Software ein Programm, welches die offizielle Definition der „Open Source Inititative" (OSI) erfüllt, die aus 10 Kriterien besteht.[21] Dazu gehört neben der Verfügbarkeit des Quelltextes auch das Recht zur freien Vervielfältigung, Verbreitung und Bearbeitung durch jedermann.[22] Der Begriff OpenSource Software löste Ende der 90er durch diese Definition den unpräzisen Begriff der „Freien Software" ab. Unter OpenSource kann man ferner auch eine Philosophie für die Entwicklung von Software verstehen.[23]

---

[16] http://www.common-pki.org/ oder Wikipedia, Common PKI, Version vom 11.10.2009, 20.35 Uhr, http://de.wikipedia.org/w/index.php?title=Common_PKI&oldid=65481471.

[17] H. B. Wabnitz / T. Jonovsky, Rn. 59; Wikipedia, Makro, Version vom 25.11.2009, 06.29 Uhr, http://de.wikipedia.org/w/index.php?title=Makro&oldid=67236521.

[18] http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=43485 (16.12.2009).

[19] Wikipedia, OpenDocument, Version vom 07.12.2009, 22.17 Uhr, http://de.wikipedia.org/w/index.php?title=OpenDocument&oldid=67729326.

[20] Quelltext ist der in einer Programmiersprache verfasste Text eines Computerprogramms, welcher das Programm formal beschreibt und durch einmalige Übersetzung in eine ausführbare Software verwandelt wird. Siehe dazu auch Wikipedia, Quelltext, Version vom 19.11.2009, 09.20 Uhr, http://de.wikipedia.org/w/index.php?title=Quelltext&oldid=66997681.

[21] V. Sauer / B. Henzelmann, S. 5 ff.

[22] A. Metzger / T. Jaeger, GRUR 1999, S. 841.

[23] E. S. Raymond.

OSCI

Abkürzung von „Online Services Computer Interface“. Es handelt sich dabei um eine von der OSCI-Leitstelle entwickelte Protokollfamilie für eGovernment-Anwendungen.[24] Mit dem zum OSCI-Standard gehörenden Protokoll „OSCI-Transport“ werden die klassischen Schutzziele Integrität, Authentizität, Vertraulichkeit und Nachvollziehbarkeit bei der Übermittlung von Nachrichten gewährleistet. OSCI basiert auf XML.[25]

PDF

Abkürzung von „Portable Document Format“. Es handelt sich um ein von der Firma Adobe aus dem ebenfalls von Adobe entwickelten Seitenbeschreibungsstandard „Postscript“ weiter entwickeltes, universelles Dateiformat für den Austausch digitaler Dokumente zwischen allen Betriebssystemen.[26] Seit PDF Version 1.1 lassen sich PDF-Dokumente mit einem Passwort schützen. Mit der Version 5 des Programms „Acrobat“ (vom Hersteller Adobe) unterstützen PDF-Dokumente auch das Signieren und Verschlüsseln mittels Public-Key-Verfahren[27] wie im Signaturgesetz (SigG) spezifiziert.

Positive Empfangsbestätigung

Empfangsbestätigung, die ein Absender elektronischer Gerichtspost erhält, wenn das Gericht die elektronische Gerichtspost formatgerecht erhalten hat. Beim Elektronischen Gerichts- und Verwaltungspostfach (EGVP) wird dem Absender stets automatisch eine Eingangsbestätigung übermittelt, so dass der Absender den ordnungsgemäßen Zugang seines abgesandten Dokuments bei Gericht sofort überprüfen kann.[28]

RTF

Abkürzung für „Rich Text Format“. Ein durch die Firma Microsoft entworfener, offener Standard für die Codierung von formatierten Texten und Grafiken für den Austausch von entsprechenden Dateien zwischen verschiedenen Textverarbeitungsprogrammen. Die interne Codierung der Daten und Metadaten einer RTF-Datei ist ASCII.[29]

S/MIME

Abkürzung für „Secure / Multipurpose Internet Mail Extensions“. MIME ist dabei ein Standard,[30] der unter anderem den Aufbau von E-Mails festlegt.[31] MIME ermöglicht z.B. den Versand von Datei-Anhängen an Text-E-Mails. Der Standard S/MIME erweitert den MIME-Standard um Konstrukte für signierte (zur Wahrung der Authentizität) und verschlüsselte (zur Wahrung der Vertraulichkeit) Nachrichtenformate.[32] Der

[24] S. Mehlich, S. 154.
[25] http://www1.osci.de/sixcms/detail.php?gsid=bremen02.c.1160.de (16.12.2009).
[26] T. Merz / O. Drümmer, S. 1.
[27] T. Merz / O. Drümmer, S. 559 ff.
[28] Vgl. W. Viefhues, NJW 2005, S. 1010.
[29] Microsoft, S. 7.
[30] http://www.ietf.org/html.charters/smime-charter.html (16.12.2009).
[31] E. Levinson; siehe auch A. S. Tanenbaum, S. 649.
[32] J. Schwenk, S. 63 ff.

Standard bietet ferner auch flexible Methoden zur Authentifizierung und Nichtabstreitbarkeit und kann mit verschiedenen kryptographischen Standards wie PGP oder X.509 verwendet werden.[33]

SMTP

„Simple Mail Transfer Protokoll" ist ein IETF-Standard, der die Übertragung (Weiterleitung) von E-Mails zwischen dem Sender und dem Empfänger (-Postfach) regelt.[34] SMTP selbst ist ein Protokoll, welches nur ASCII-Daten übertragen kann. Zur Weiterleitung von (nicht-ASCII) Dateien über das SMTP-Protokoll wird der MIME-Standard verwendet. S/MIME kann zur sicheren Ende-zu-Ende-E-Mail-Kommunikation verwendet werden.

SSL/TLS

Secure Sockets Layer (SSL) oder Transport Layer Security (TLS)[35] sind Protokolle, welche als Hauptaufgabe die Sicherstellung der Vertraulichkeit und Integrität (durch Verschlüsselung und Signierung) sowie die Authentifikation der Kommunikationspartner bei Ende-zu-Ende-Verbindungen im Internet haben.[36] TLS ist dabei die neueste, standardisierte[37] Weiterentwicklung von SSL. Daher wird TLS z.T. auch als SSL Version 3.1 bezeichnet.[38] Weder SSL noch TLS sind selbst Nutzdaten übertragende Protokolle. Sie dienen nur zur Besicherung anderer Nutzdatenprotokolle wie z.B. HTTP oder SMTP.

TIFF

Abkürzung für „Tagged Image File Format". Ein von der Firma Adobe entwickeltes Dateiformat zur Speicherung von ein- oder mehrseitigen, farbigen oder schwarzweißen Bilddaten. Es eignet sich für die Speicherung und Verarbeitung von Daten von Scannern, Faxgeräten, Kameras oder Bildverarbeitungsprogrammen.[39] Die Verarbeitung von Text ist nicht der Fokus von TIFF. Das Format eignet sich beim Dokumentenaustausch in erster Linie für eingescannte Anlagen, weniger für die Schriftsätze als solche.

Unicode

ist ein universeller, multilingualer Standard[40] zur Codierung von Zeichen und Text. Er enthält derzeit 99.024 verschiedene Zeichen und löst veraltete Standards wie ASCII bei der Darstellung und Übertragung von Informationen über weltweite Telekommunikationsnetze ab.[41]

---

[33] A. S. Tanenbaum, S. 867.
[34] C. Eckert, S. 145; A. S. Tanenbaum, S. 655 ff.
[35] T. Dierks.
[36] C. Eckert, S. 729 ff.
[37] http://www.ietf.org/html.charters/tls-charter.html (16.12.2009).
[38] A. S. Tanenbaum, S. 879 f.
[39] Adobe Developers Association, S. 4.
[40] http://www.unicode.org (16.12.2009).
[41] J. Aliprand, S. 1.

X-Justiz

ist ein von der Bund-Länder-Kommission entwickelter, auf XML basierender Justizdatensatz zum Datenaustausch von Dokumenten.[42] Im Standard werden Datenfelder definiert, die den Austausch möglichst vieler verfahrensrelevanter Daten ermöglichen sollen.[43] X-Justiz wird z.B. für Registergerichte als X-Register und für Notare als X-Notar konkretisiert.[44]

XML

Abkürzung für „Extensible Markup Language". Ein durch das W3C-Konsortium[45] standardisiertes,[46] menschenlesbares Dateiformat zur strukturierten Speicherung beliebiger Computerdaten sowie deren Austausch über Computernetze wie dem Internet.[47] Mit XML können sowohl Inhalte als auch Struktur der Informationen definiert werden, ohne dass man durch eine vorgegebene Menge von Sprachelementen beschränkt wird.[48] Im Gegensatz zu HTML, dessen Fokus die Beschreibung von Seiten des WWW ist, kann XML somit beliebige Daten beschreiben.[49]

zip

ist ein offenes Format zur komprimierten Archivierung von Dateien. Neben mehreren Dateien können auch ganze Verzeichnisbäume in einer einzelnen ZIP-Datei archiviert und komprimiert werden. Die Archivdateien tragen üblicherweise die Endung .zip.[50]

D. Schrifttum

I. Monographien und Beiträge in Sammelwerken

Adobe Developers Association, TIFF Specification Revision 6.0, Juni 1992, http://partners.adobe.com/public/developer/tiff/index.html (16.12.2009).

Joan Aliprand, The Unicode Standard Version 5.0. Addison-Wesley, 2007.

Tim Berners-Lee, Information Management: A Proposal, CERN, Geneva, Switzerland, März 1989, http://www.w3.org/History/1989/proposal.html (16.12.2009).

Tim Berners-Lee, / D. Connolly, Hypertext Markup Language – 2.0. IETF RFC 1866, November 1995, http://www.ietf.org/rfc/rfc1866.txt (16.12.2009).

[42] H. Radke, JurPC Web-Dok. 46/2006, Rn. 1 ff.
[43] http://www.xjustiz.de/ (16.12.2009).
[44] J. Bettendorf, Rn. 156.
[45] Das World Wide Web Consortium (W3C) ist eine Organisation zur Standardisierung der Techniken des World Wide Webs.
[46] T. Bray et al.
[47] E. R. Harold / W. S. Means.
[48] J. Bettendorf, Rn. 156.
[49] A. S. Tanenbaum, S. 693.
[50] Wikipedia, ZIP (Dateiformat), Version vom 08.11.2009, 15.14 Uhr, http://de.wikipedia.org/w/index.php?title=ZIP_(Dateiformat)&oldid=66561287.

Tim Bray et al., Extensible Markup Language (XML) 1.0. September 2006, http://www.w3.org/TR/2006/REC-xml-20060816/ (16.12.2009).

Dierks, T., RFC 4346: The Transport Layer Security (TLS) Protocol, Version 1.1. IETF Network Working Group, April 2006 http://tools.ietf.org/html/rfc4346 (16.12.2009).

Claudia Eckert, IT-Sicherheit, 5. Auflage, 2008.

Günter Gall / Klaus-Dieter Rippe / Gerard Weiss, Die europäische Patentanmeldung und der PCT in Frage und Antwort, 2006.

John Klensin, RFC 2821: Simple Mail Transfer Protocol, IETF Network Working Group, April 2001 http://tools.ietf.org/html/rfc2821 (16.12.2009).

E. Levinson, RFC 2387: The MIME Multipart/Related Content-type, IETF Net-work Working Group, August 1998, http://tools.ietf.org/html/rfc2387 (16.12.2009).

Harald Mehlich, Electronic government, 2002.

Thomas Merz / Olaf Drümmer, Die PostScript- & PDF-Bibel, 2. Auflage, 2002.

Microsoft Corporation, Rich Text Format (RTF) Specification Version 1.9.1., März 2008.

David A. Patterson / John L. Hennessy, Computer Organization & Design, 2. Auflage, MK Morgan Kaufmann, 1998.

Hermann-Josef Piepenbrock, Wolfgang Büchner et al. (Hrsg.), Beckscher TKG-Kommentar. 2. Auflage, 2000, Teil C, Glossar.

E.S. Raymond, The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary, Sebastopol, CA, USA: O'Reilly & Associates Inc., 2001, http://catb.org/~esr/writings/cathedral-bazaar/cathedral-bazaar/ (16.12.2009).

G.S. Robinson / C. Cargill, History and impact of computer standards. IEEE Computer, Volume 29, Oktober 1996, Nr. 10, S. 79-85.

Eliotte Harold Rusty / W. Scott Means, XML in a Nutshell, OReilly, 2002.

Jörg Schwenk, Sicherheit und Kryptographie im Internet: Von sicherer e-mail bis zu IP-verschlüsselung, 2005.

Andrew S. Tanenbaum, Computernetzwerke, 4. Auflage, Prentice Hall, 2003.

Volker Sauer / Bettina Henzelmann, OpenSource aus ökonomischer Sicht. Seminararbeit am Fachgebiet Information Systems der TU Darmstadt, November 2006, http://www.volker-sauer.de/henzelmann_sauer_-OS_aus_oek._sicht.pdf (06.08.2008).

Heinz-Bernd Wabnitz / Thomas Jonovsky, Handbuch des Wirtschafts- und Steuerstrafrechts, 3. Auflage, 2007.

II. Beiträge in Zeitschriften

K. Bacher, Elektronisch eingereichte Schriftsätze im Zivilprozess, NJW 2009, S. 1548.

Bundesministerium für Wirtschaft, Interoperabilitätsstandard für elektronische Signaturen. MMR 2001, Nr. 10, XVIII.

A.H. Horns, Anmerkungen zu begrifflichen Fragen des Softwareschutzes. GRUR, 2001, S. 14.

A. Metzger / T. Jaeger, Open Source Software und deutsches Urheberrecht. GRUR, 1999, S. 839.

H. Radke, eJustice - Aufbruch in die digitale Epoche. JurPC Web-Dok. 46/2006, http://www.jurpc.de/aufsatz/20060046.htm (14.12.2009).

W. Viefhues, Das Gesetz über die Verwendung elektronischer Kommunikationsformen in der Justiz, NJW 2005, S. 1009.

H. Vieregge, Aktuelle Berichte - April 2004. GRUR, S. 304.